United States District Court

NORTHERN DISTRICT OF CALIFORNIA

FILED
2010 NOV -8 P 5:03
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
N.D. OF CA-SAN JOSE

UNITED STATES OF AMERICA

V.

Rachel OCHOA

SEALED BY ORDER OF THE COURT

CRIMINAL COMPLAINT

10-70946 PVT

CASE NUMBER:

I, the undersigned complainant, being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about and between, 2005 and 2009, in Santa Clara County in the Northern District of California defendant(s), (Track Statutory Language of Offense)

Stole and converted to her own use and the use of another, and without authority conveyed to another, a thing of value of the United States and a department and agency thereof, namely at least five social security numbers and cards

in violation of Title 18 United States Code, Section(s) 641
I further state that I am a(n) Special Agent (Official Title) and that this complaint is based on the following facts:

SEE ATTACHED AFFIDAVIT

MAXIMUM PENALTIES: up to 10 years imprisonment, $250,000.00 fine, 3 years TSR, $100 SAF

REQUESTED PROCESS/BAIL: No bail warrant

APPROVED AS TO FORM: _____
ASSISTANT UNITED STATES ATTORNEY

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

_____
Signature of Complainant

Sworn to before me and subscribed in my presence,

Nov. 8, 2010 (Date) at San Jose, California (City and State)

Patricia V. Trumbull
United States Magistrate Judge
Name & Title of Judicial Officer

_____
Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH AND ARREST WARRANTS AND CRIMINAL COMPLAINT

I, Gregory S. Fine, a Special Agent with the Federal Bureau of Investigation ("FBI"), being first duly sworn, hereby depose and state as follows:

A. Introduction and Agent Background

1. I make this affidavit in support of an application for: (1) a criminal complaint, (2) a search warrant, and (3) an arrest warrant, based on the following information concerning the theft and sales of United States' property. The arrest warrant is for:

- Rachel Ochoa ("OCHOA"), born [redacted], who resides at [redacted]. The facts set forth in this affidavit establish that there is probable cause to believe that OCHOA is guilty of theft of government property.

The search warrant application seeks authorization to search the locations set forth below, including:

- OCHOA's office space at the Social Security Administration office located at 2500 Fontaine Road, San Jose, California;
- OCHOA's residence at [redacted];
- OCHOA's personal cellular telephone(s)[1];

each of which is more fully described in Attachment A, for documents, records, materials, and items relating to violations of Title 18, United States Code, Section 641 (theft of government property). In relevant part, Section 641 punishes anyone who embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof.

---

[1] At this time, the type of Ochoa's cellular telephone is unknown. Therefore, out of an abundance of caution, this application for a search warrant will treat her cellular telephone as being a "computer," that is, having access to the Internet and being capable of containing and storing electronic media. For these reasons, this affidavit contains the relevant "computer search protocol" language and Attachment C, even though this warrant does not seek permission to search any desktop, laptop, or personal computer.

2. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint and search and arrest warrants, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that a crime was committed by OCHOA and that evidence of the above-referenced violations will be located in the premises described in Attachment A.

3. I am a Special Agent with the Federal Bureau of Investigation (FBI) . I have been employed as a Special Agent since September 2006, and am presently assigned to the white collar crime squad in the San Jose Resident Agency Office of the San Francisco Division of the FBI. As a Special Agent, I am authorized to investigate crimes involving public corruption, wire fraud, money laundering, mail fraud, securities fraud, and other complex crimes. I have successfully completed 18 weeks of criminal investigative training at the FBI Academy in Quantico, Virginia, which included training on investigating public corruption and financial crime. Through my training and experience, as well as discussions with other agents, I have become knowledgeable in the methods employed to commit fraudulent crimes. The information set forth in this affidavit is based on my personal knowledge and that which has been provided to me by other agents with whom I have been working on this ongoing investigation.

B. History of Investigation and Facts Supporting Probable Cause

4. In April 2009, the FBI received information from an individual (hereafter "Source") regarding a corrupt Social Security Administration ("SSA") employee. Source described his/her own experience attempting to purchase a legitimate social security card from this individual, known to the Source as the mother of Chato Ochoa and Aurora Ochoa. Source was in the process of purchasing a legitimate social security card from Chato and Aurora Ochoa's mother, for approximately $2,500, when Source was arrested on identity theft charges. After Source's arrest and conviction, Source no longer had the same access to the Source's associates that would have been necessary for Source to purchase the social security card. In addition to the above-referenced criminal conviction, the Source also has several juvenile adjudications and adult felony convictions.

5. Source was unable to provide a detailed description of OCHOA, but did provide

the following description of Aurora Ochoa: Source stated that Aurora Ochoa was currently serving time for burglary at the Valley State Prison for Women. Additionally, Source believed that Aurora Ochoa's mother worked at the Social Security Administration office in San Jose, California, near Fontaine Street.

6. After checking Valley State Prison for Women records, I confirmed that Aurora Ochoa's mother is Rachel OCHOA. OCHOA resides at [redacted] Moreover, I confirmed with the Social Security Administration - Office of the Inspector General ("SSA-OIG") that the same Rachel OCHOA is employed by the Social Security Administration, and currently works at the Social Security office located at 2500 Fontaine Road, San Jose, California. SSA-OIG confirmed that OCHOA is employed in a position that enables her to issue social security cards.

7. Through the additional investigation described below, including an audit of the social security cards issued by OCHOA, and several witness interviews, I discovered evidence supporting the allegation that OCHOA has been, in fact, fraudulently issuing social security cards. OCHOA's fraudulent actions included improperly stealing social security numbers and cards from the United States government and having the cards mailed to ineligible recipients. These recipients have paid thousands of dollars in order to obtain the cards.

C. The SSA-OIG Audit

8. In order to determine whether OCHOA was fraudulently issuing social security cards, SSA-OIG produced an audit report containing all of the social security cards issued by OCHOA in the last five years. The audit report included personal information for each individual (hereinafter referred to as "card-recipient") who was issued a social security card by OCHOA. SSA-OIG knew that all of the cards listed on the report were issued by OCHOA because OCHOA was required to provide a unique personal identification number and password before accessing the Social Security Administration's computer system. The audit report only included cards issued under OCHOA's personal identification number. The report also identified the documentation each card-recipient allegedly provided to OCHOA in order to substantiate his/her claim that he/she was legally eligible to receive a social security card.

9. The audit report showed that a large number of card-recipients provided OCHOA with an alien identification number ("A-number"). By entering this documentation into the SSA's computer system, OCHOA was representing to the SSA that she had reviewed the documentation and was satisfied that it substantiated the card-recipient's identity and work eligibility in the United States.

10. SSA has mandatory protocol regarding verification of A-numbers. SSA employees must confirm each A-number using a secured website maintained by the Department of Homeland Security. During the audit of OCHOA's work, SSA-OIG used that website, the same website that OCHOA should have used, to verify the A-numbers. By entering the A-numbers into this website, SSA-OIG discovered dozens of instances in which the A-number that OCHOA allegedly verified prior to issuing a social security card either belonged to an unrelated third party or was not a valid A-number. In each of these instances, OCHOA should not have issued a social security card. It appears OCHOA ignored these legal requirements and issued social security cards anyway.

11. Additionally, as part of its investigation, SSA-OIG requested to review the applications associated with the improperly issued social security cards. SSA-OIG discovered that many of the applications simply did not exist. As part of the Social Security Administration's regulations, all applicants requesting a new social security card must physically visit a Social Security Administration office and complete an application. Not one of OCHOA's card-recipients should have been issued a card without first completing an application.

D. OCHOA's Card-Recipients

12. The FBI and SSA-OIG interviewed several card-recipients identified in the audit report. Often, the card-recipients admitted that he/she had not visited an SSA office to apply for and receive a social security card. Rather, most card-recipients purchased their cards in cash from a variety of sources. Many card-recipients also admitted that they were not legally eligible to receive a social security card, and would not have been able to obtain a social security card had they followed the standard application process. Below is a summary, in sum and substance, of a few card-recipient interviews:

a. Card-recipient G.R.

13. In approximately late-2008, while visiting a friend's house, G.R. was introduced to a person named Valtazar. (G.R. does not know whether Valtazar is a first or last name.) G.R. is an undocumented individual who resides in San Jose, California. Valtazar told G.R. that Valtazar could get a legitimate social security card for G.R., if G.R. paid Valtazar $4,300 in cash. G.R. trusted Valtazar, but does not specifically recall why G.R. believed Valtazar could, in fact, obtain a valid social security card. Immediately, G.R. left the friend's house and withdrew $4,300 in cash. Then, G.R. returned to the friend's house and paid Valtazar the cash. In order to obtain the card, Valtazar told G.R. to provide Valtazar with G.R.'s full name, date of birth, and address.

14. Approximately six or seven months later, G.R. received a valid social security card in the mail at the address G.R. had provided to Valtazar. To G.R., the envelope appeared official and to have been sent directly from the Social Security Administration. SSA records confirm that G.R.'s card was issued on May 28, 2009 and mailed shortly thereafter.

15. G.R. was one of the few individuals identified in the SSA-OIG audit report for which an application existed. During the interview, FBI and SSA-OIG agents showed G.R. this application. G.R. confirmed that the name, date of birth, and address were accurate. However, G.R. stated that the signature on the application was not G.R.'s signature. Additionally, G.R. confirmed that the A-number and Mexican passport number listed on the application did not belong to G.R. In fact, G.R. did not possess an A-number nor a Mexican passport.

16. Also on the application, in the section entitled "FOR SSA USE ONLY," OCHOA's signature appears as the employee who reviewed evidence and/or conducted the interview. Additionally, "Yes" was entered under the section labeled "IN-PERSON INTERVIEW CONDUCTED?" Despite these representations by OCHOA, G.R. confirmed that G.R. had never visited an SSA office, never provided any documentation related to G.R.'s identity, and was never interviewed by OCHOA during the application process.

b. Card-recipient J.F.

17. Approximately five years ago, while working on a construction job in Hayward,

California, J.F had a conversation with "Sergio" about how to obtain a legitimate social security card. (J.F. assumes Sergio is a first name, but does not know Sergio's last name.) J.F., an undocumented individual, could not obtain a social security card through a legitimate application process. Sergio told J.F. that Sergio knew someone named "Guillermo." Sergio said that Guillermo could help J.F. obtain a social security card. Sergio provided J.F. with Guillermo's contact information. J.F. contacted Guillermo and arranged a meeting at a commercial building in San Jose. Guillermo told J.F. that it would cost $2,600 to purchase a social security card. Guillermo told J.F. that half of that fee was due in cash immediately and the other half was due when J.F. received the card. Following Guillermo's instructions, J.F. provided Guillermo with J.F.'s personal information, including J.F's name and date of birth.

18. For approximately two years, J.F. waited for but never received the social security card. J.F. frequently called Guillermo to ask about the status of the card. Guillermo told J.F. the process would take more time. Eventually, Guillermo called J.F. to say that the social security card was ready. J.F. met Guillermo at a street intersection in Milpitas, California and paid Guillermo the remaining $1,300 in cash for the social security card. Guillermo gave J.F. a social security card.

19. SSA records confirm that, on March 6, 2008, a social security card was issued to J.F. and mailed shortly thereafter. SSA-OIG requested to review J.F.'s social security card application, but discovered that an application does not exist. Despite the absence of an application, and through the audit report, SSA can conclude that OCHOA correctly entered J.F.'s name and date of birth into the SSA's computer system. The audit report also confirms that OCHOA claimed to have reviewed an A-number before issuing the card. Importantly, that A-number does not belong to J.F.

c. Card-recipient A.V.

20. Approximately five years ago, A.V. wanted to obtain a legitimate social security card, but since A.V. is an undocumented individual, A.V. is not legally entitled to receive such a card. Around that time, A.V. approached an individual at an unknown location and asked that individual about getting a social security number. A.V. recalls that A.V. paid this individual for

a social security card, but does not remember the individual nor the exact amount that was paid.

21. A.V. does not recall how long it took to receive the social security card, but recalls that it arrived in the mail. Official SSA records confirm that the card was issued on April 15, 2005 and mailed to an address in San Jose, California shortly thereafter.

22. SSA-OIG, through the audit report, concluded that OCHOA issued the card to A.V. SSA-OIG reviewed its records and determined that no application exists for A.V. The personal information, including name, date of birth, and address, entered by OCHOA into SSA's computer system for A.V. is correct. However, OCHOA allegedly reviewed a document during the application process that included A.V.'s A-number. This A-number does not belong to A.V. Additionally, A.V. confirmed that this transaction did not occur at an SSA office, that A.V. did not fill out any government forms, and that A.V. did not show any immigration or identity documents to anyone, including an individual named OCHOA. If A.V. had legitimately applied for a social security card, A.V. would have been denied.

d. Card-recipient J.P.

23. Several years ago, J.P. wanted to obtain a social security card, but knew that J.P. was not legally entitled to receive one. J.P. obtained a social security card from an individual at a real estate office in San Jose, California. This real estate office no longer exists. J.P. recalls paying this individual, but does not remember exactly how much. J.P. recalls that due to the amount of money, J.P. was confident that the card would be legitimate as opposed to counterfeit. J.P. never visited an SSA office to apply for the card. Additionally, J.P. confirmed that J.P. never showed any SSA official any immigration or identity documents, nor did J.P. complete any application forms. J.P. received a social security card in the mail, but does not recall precisely when the card arrived. SSA records confirm that SSA issued J.P.'s card on March 29, 2007 and mailed the card shortly thereafter.

24. SSA-OIG, through a review of the audit report, confirmed that J.P.'s social security card was issued by OCHOA. SSA-OIG was unable to locate an application for J.P. The personal information entered by OCHOA into the SSA's computer system for J.P. is correct, but the A-number from the documentation allegedly reviewed by OCHOA does not belong to J.P.

e. Card-recipient J.M.

25. Approximately two years ago, J.M. walked into the Tropicana Market in San Jose, California and asked an unknown individual how J.M. could obtain a social security card. Since J.M. is illegally residing in the United States, J.M. is not legally entitled to receive a social security card. J.M. paid the individual $5,000 in cash, confirming J.M.'s belief that the social security card would be legitimate. J.M. knew that counterfeit social security cards could be purchased at the Tropicana Market, but for far less money.

26. Through the audit report, SSA-OIG confirmed that OCHOA entered and issued J.M.'s social security card. In SSA's computer system, OCHOA correctly entered J.M.'s name, date of birth, and address. J.M. recalls filling out a form, that appeared to be a legitimate government form, with personal information and handing that form to the individual at the Tropicana Market. However, SSA-OIG determined that no application exists in the SSA's records for J.M. Additionally, the A-number for the documentation that OCHOA allegedly reviewed does not belong to J.M.

27. Approximately one year after paying for the card at the Tropicana Market, J.M. received a legitimate social security card in the mail. Official SSA records confirm that the card was issued on December 3, 2008 and mailed shortly thereafter.

28. In each of the above referenced examples, OCHOA entered into the SSA's computer system a request to issue a new social security card to ineligible card-recipients. In furtherance of her scheme, OCHOA falsely claimed that the card-recipients presented OCHOA with various identification documents. OCHOA entered false A-numbers to support each card-recipient's entitlement claim to a social security card. In reality, none of the above card-recipients were ever interviewed by OCHOA. Also, none of the card-recipients entered a Social Security Administration office, as is required to obtain a new social security card. In fact, all of the card-recipients are undocumented individuals, residing in the United States illegally, and are not eligible to receive a social security card. OCHOA's fraudulent entries and representations caused SSA to issue social security cards and to mail the cards to the card-recipients.

E. Financial Analysis of OCHOA's Bank Accounts

29. In order to establish whether OCHOA was receiving financial compensation from card-recipients, a financial analysis was conducted of OCHOA's bank accounts at Bank of America. Since 2005, OCHOA has maintained at least five different bank accounts at Bank of America. All of her bank accounts show the same pattern of activity. That is, any monies deposited into OCHOA's bank accounts are quickly withdrawn in cash.

30. OCHOA's bank accounts demonstrate that she maintains two major sources of income. The first source of income is her SSA salary. The second source of income is retirement income from the State of California. OCHOA withdraws nearly all of this income from her bank accounts in cash almost immediately after it is deposited. With her remaining balance, OCHOA pays a small number of bills directly from her accounts, including payments to Pacific Gas & Electric, SBC, Comcast, and Nextel Communications. (In order to cover these payments, OCHOA occasionally deposits a small amount of cash, $1,000 or less, back into her accounts. However, OCHOA does not maintain an account balance greater than is required to pay these bills.) From this, it appears that most of OCHOA's daily transactions, occurring outside of her bank, are cash transactions. Based on my training and experience, I know that dealing mostly in cash transactions is a typical behavior of subjects who wish to conceal a source of their income and assets, and also conceal monetary transactions from law enforcement.

F. Search Locations

31. Based upon the above information, I believe that probable cause exists to believe that OCHOA has violated Title 18, United States Code, Section 641 (theft of government property) and that evidence, fruits, and instrumentalities of these violations will be found on OCHOA's person, at OCHOA's work office space, OCHOA's residence, and stored on any personal cellular telephones maintained by OCHOA, each of which is more fully described in Attachment A.

32. OCHOA works at the Social Security Administration office located at 2500 Fontaine Road, San Jose, California. In order to issue social security cards, and further the above-described scheme, OCHOA must conduct many of these activities at her office, in and

around her office space, desk, and work area.

33. OCHOA resides at [redacted]. OCHOA's Department of Motor Vehicles record and her above-described Bank of America statements both confirm that this is her residence. Finally, as stated above, Valley State Prison for Women records confirmed that [redacted] is OCHOA's residence.

34. Based upon my training and experience, I believe evidence of the referenced violations will not only be found at OCHOA's work location, but also on OCHOA's person, at OCHOA's residence, and on OCHOA's cellular telephone(s), all more fully described in Attachment A. This is because subjects committing fraudulent crimes at their place of employment, typically store evidence, fruits, and instrumentalities of their violations in locations other than their place of employment in order to avoid detection at work and to avoid losing their job. Through my training and experience, I know that these subjects may instead store evidence of their crimes in their residence and on their personal cellular telephone. Additionally, the nature of the above described scheme may require OCHOA to carry evidence, fruits, and instrumentalities on her person or on cellular telephones in order to move these items between her residence and work location.

G. Background regarding computers, the Internet, and E-Mail

35. The term "computer" as used herein is defined in 18 U.S.C. § 1030(e)(1), and includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

36. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know the following:

37. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

38. Internet Service Providers ("ISPs"): Most individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs").

39. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods;

40. Internet Protocol Address ("IP address"): An Internet Protocol address is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots (e.g., 149.101.10.40). Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet service providers ("ISPs") assign IP addresses to their customers' computers. An ISP might assign a different IP address to a customer each time the customer makes an Internet connection (so-called "dynamic IP addressing"), or it might assign an IP address to a customer permanently or for a fixed period of time (so-called "static IP addressing"). The IP address used by a computer attached to the Internet is unique for the duration of a particular session; that is, from connection to disconnection. ISP's typically log their customers' connections, which means that the ISP can identify which of their customers was assigned a specific IP address during a particular session.

41. E-mail is a popular form of transmitting messages and/or files in an electronic environment between computer users. A server is a computer that is attached to a dedicated network and serves many users. An e-mail server may allow users to post and read messages and to communicate via electronic means. When an individual computer user sends e-mail, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination;

42. Any e-mail that is sent to a subscriber is stored in the subscriber's "mail box" on the provider's servers until the subscriber deletes the e-mail or the subscriber's mailbox exceeds the storage limits preset by the e-mail provider. If the message is not deleted by the

subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on the provider's servers indefinitely;

43. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to the servers of the e-mail provider, and then transmitted to its end destination. Users have the option of saving a copy of the e-mail sent. Unless the user specifically deletes the e-mail from the e-mail account, the e-mail can remain on the system indefinitely. The sender can delete the stored e-mail message thereby eliminating it from the e-mail box maintained at the e-mail provider, but that message will remain in the recipient's e-mail box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations;

44. A subscriber can store files, including e-mails and image files, on servers maintained and/or owned by the e-mail provider; and

45. E-mails and image files stored on a e-mail provider server by a subscriber may not necessarily be located in the subscriber's home computer. The subscriber may store e-mails and/or other files on the provider's server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files that the subscriber has stored on the e-mail provider's server.

46. Data that is processed by a computer may be written to the computer's internal hard drive or other storage medium even if the user does not intentionally save the information. Other storage medium may include compact discs (CDs), digital video disks (DVDs), floppy diskettes, thumb drives, pocket hard drives, external hard drives and flash drives. For example, a computer operating system may take random data out of working memory and use it to "pad" files on a computer hard drive during the storage process.

47. Electronic information can remain on computer storage media, such as internal and external hard drives, pocket drives, thumb drives, CDs, DVDs, diskettes, and flash drives, for an indefinite period of time. Even when a computer user attempts to delete records from a computer storage medium, the records may still exist and be recovered through computer

forensic techniques.

48. Computer files may be easily moved from computer to computer, using direct wire connections or through the use of storage media such as floppy diskettes, CDs, DVDs, diskettes, thumb drives, pocket drives, flash drives and USB drives.

H. Search and Seizure Procedures Pertaining to Computers

Search of Computers and Computer Records

49. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that during the search of premises it is not always possible to search computer equipment and storage devices, specifically cellular telephone storage devices and equipment, for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, it may be possible for the search team to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. For example, the search team may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a warrant. Similarly, the search team may be able to locate the materials covered in the warrant by looking for particular directory or file names. In other cases, however, such techniques may not yield the evidence described in the warrant. Computer users can mislabel or hide files and directories; encode communications to avoid using key words; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for

information. These steps may require the search team to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the warrant.

c. Searching computer systems requires the use of precise, scientific procedures, which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

d. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing fifteen gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 7.5 million pages of data, which if printed out, would completely fill a 10' x 12' x 10' room to the ceiling.

e. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard" is necessary to decrypt the data into readable form. Computer users also can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a

computer user can conceal text in an image file, which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

Search of Digital Media in Light of the Ninth Circuit's Ruling in CDT.

50. No search or seizure shall occur of any devices or media that store data electronically except as set forth in Attachment C. Moreover, this application seeks permission only to search OCHOA's personal cellular telephone(s). In executing the search warrant authorized by this Court's order, the following protocols will apply:

a. In executing this warrant, the government must begin by ascertaining whether all or part of a search of a device or media that stores data electronically (collectively, the "device" or "cellular telephone") that is authorized by this warrant reasonably can be completed at the site within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if authorized by law because removal is (1) necessary to preserve evidence, or (2) if the item is contraband, a forfeitable instrumentality of the crime, or fruit of crime.

b. If the government determines that a reasonable search as authorized in this warrant cannot be completed at the site within a reasonable period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then completing the search of the mirror image off site (e.g., at a computer crime laboratory).

c. The government may remove from the search location a device only if the device cannot be searched reasonably on site, or by mirror-imaging or otherwise duplicating its contents for off site examination – unless authorized by law to remove the device because (1) removing the device is necessary to preserve evidence, or (2) the device is contraband, a forfeitable instrumentality of the crime, or fruit of crime. The government also may remove from the site any related equipment (e.g., keyboards or printers) or documents (e.g., system operating or software manuals) that reasonably appear to be necessary to conduct an off-site search of a

device in which data is stored electronically.

e. If the government removes a device or related equipment or documents from the place they were found in order to complete the search off-site, within ten calendar days of the removal the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents.

f. The government must complete an off-site search of a device that agents removed in order to search for evidence of crime, as promptly as practicable and no later than 30 calendar days after the initial execution of the warrant. The government must complete an off-site search of any mirror image of any device in which data is stored electronically as promptly as practicable and no later than 120 calendar days after the initial execution of the warrant. Within thirty calendar days after completing an off-site search of a device pursuant to this warrant, the government must return any device, as well as any related equipment or document that was removed from the site in order to complete the search, unless, under the law, the government may retain the device, equipment, or document (1) to preserve evidence, or (2) because the device, equipment, or document is contraband, a forfeitable instrumentality of the crime, or fruit of crime. Within a reasonable period, not to exceed sixty calendar days after completing the authorized search of a device or image, the government also must use reasonable efforts to destroy – and to delete from any devices or storage media or copies that it has retained or made – copies of any data that are outside the scope of the warrant but that were copied or accessed during the search process, unless, under the law, the government may retain the copies (1) to preserve evidence, or (2) because the copies are contraband, a forfeitable instrumentality of the crime, or fruit of crime. The deadlines set forth in this paragraph may be extended by court order for good cause shown.

g. In conducting the search authorized by this warrant, whether on site or off site, the government must make all reasonable efforts to use methods and procedures that will locate and expose only those categories of files, documents, or other electronically stored information that are identified with particularity in the warrant while, to the extent reasonably practicable, minimizing exposure or examination of irrelevant, privileged, or confidential files.

h. The terms of this warrant do not limit or displace any person's right to file a motion for return of property under F.R.Cr.P. 41(g). Nor does the issuance of this warrant preclude any person with any interest in any seized item from asking the government to return the item or a copy of it.

i. The government must promptly notify the judge who authorized issuance of the search warrant (or, if that judge is unavailable, to the general duty judge) if a dispute arises about rights or interests in any seized or searched item – or any data contained in any searched or seized item – and that dispute cannot be resolved informally. The government must deliver a copy of this written notification to any person known to assert any such right or interest.

j. Except as provided below, all search, review, and/or forensic analysis of the data on any device or mirror image authorized to be searched by this warrant (1) shall be conducted only by law enforcement personnel or other government personnel or retained forensic examiners who are not involved in the investigation of the crimes described in the affidavit (the "filter team"), and (2) shall be conducted using search protocols directed exclusively to the identification, segregation and extraction of data within the scope of this warrant. The filter team will not communicate to the law enforcement personnel, retained examiners and experts, prosecutors and any others involved in the investigation of the crimes described in the affidavit (the "investigating team") any information learned during the analysis that is outside the scope of the warrant, but may communicate to the investigating team any information or data that is within the scope of the warrant. In the event that a member of the filter team identifies information pertaining to crimes outside the scope of the warrant, such information will not be disclosed to the investigating team or used in any way absent further judicial authorization or unless a new warrant is obtained to search for such information. A new warrant may be sought by a member of the filter team, if he or she is a sworn federal agent, or by an agent not part of the investigating team. A federal prosecutor apart from the investigating team will be assigned to assist in determining whether to apply for a new warrant and in obtaining such a warrant. Absent a new warrant, the filter team will only search for and seize data that they would be entitled to retain independent of the new information and the investigating team will not use any data outside the

scope of this warrant even if found in plain view absent further judicial authorization.

I. Permission to Seize Cellular Telephones, Equipment, and Peripherals

51. In this application, I am seeking permission to seize, in accordance with the procedures described above, specifically in subsection H, OCHOA's personal cellular telephone(s). I have consulted with FBI Information Technology Specialist - Forensic Examiner (ITS-FE) Wasin Ounkeo, who has been a member of the FBI's Computer Analysis Response Team (CART) for approximately five years. ITS-FE Ounkeo is currently working at the Silicon Valley Regional Computer Forensic Laboratory, of which the FBI is a participating agency. FE Ounkeo provided me with the following information concerning cellular telephones summarized in the paragraphs below.

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a device that records still and moving images digitally. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also

include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store any digital data, such as word processing documents, even if the device is not designed to access such files. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive email. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable

storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

J. Conclusion

52. Based upon the above information, I believe that probable cause exists to believe that there have been violations of Title 18, United States Code, Section 641 (theft of government property). Furthermore, I believe that evidence, fruits, and instrumentalities of these violations will be found on or at Rachel OCHOA's person, residence, work office space, and personal cellular telephone(s) and/or in the premises more fully described in Attachment A to this affidavit. In consideration of the foregoing, I respectfully request that this court:

1) Sign the attached criminal complaint based upon the above-described probable cause;

2) Sign the attached warrant to arrest Rachel Ochoa;

3) Sign the attached warrant authorizing the requested searches (described in Attachment A) and seizures (described in Attachment B).

//

//

//

K. Request for Sealing

53. Since this investigation is continuing, disclosure of the search or arrest warrants and/or the criminal complaint, this affidavit, and/or this application and the attachments thereto will jeopardize the progress of the investigation. Accordingly, I request that the Court issue an order that the search warrant, the criminal complaint, arrest warrant, this affidavit in support of application for search warrant and criminal complaint, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

Gregory S. Fine
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
on this 8 day of November, 2010

PATRICIA V. TRUMBULL
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

1. Upon the execution of the search warrant, Rachel OCHOA's person as well as, any and all purses, bags, briefcases, luggage, boxes, mobile telephones, or any other containers on OCHOA's person or otherwise under OCHOA's immediate possession or control.

2. Rachel OCHOA's work area and other areas utilized by OCHOA at the Social Security Administration office at 2500 Fontaine Road, San Jose, California.

3. Rachel OCHOA's residence located at [redacted].

4. If not on her person, as presumed in item 1, any and all personal mobile telephones belonging to Rachel OCHOA. Any and all personal mobile telephones will be seized and searched according to the protocol described in Attachment C.

ATTACHMENT B

Items to Be Searched and Seized by Law Enforcement

The following items, from January 2005 to the present, which may be evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 641 are to be searched for and/or seized:

1. All files, including but not limited to, applications, payment records, lists, agreements, contracts, accounting records, and communications related to the issuance of social security cards.

2. All correspondence between RACHEL OCHOA and any other individual regarding the issuance of social security cards.

3. All documents related to storage facilities for which RACHEL OCHOA has access.

4. All financial records, including, but not limited to, bank statements, deposit slips, withdrawal slips, and canceled checks for RACHEL OCHOA or otherwise associated with RACHEL OCHOA.

5. All amounts of cash or monetary instruments, including, but not be limited to, cashier's checks, bank checks, certificates of deposit, credit card payment receipts, money orders, wire transfers, and personal checks.

6. All safes located within the premises.

7. All telephone billing records, including those for cell phones and other phone or fax lines.

8. All social security cards.

9. Indicia of possession of the place to be searched: consisting of articles of personal property, such as personal identification, personal correspondence, delivery pouches, diaries, checkbooks, notes, photographs, keys, utility bills, receipts, personal telephone and address books, video tapes, tending to establish the identity of the person or persons in control of the areas to be searched.

10. All cellular telephones.